DOI: https://doi.org/10.36910/6775-2524-0560-2020-41-03
УДК 004.7.056.5
[1]**Глинчук Людмила Ярославівна**, к. ф.-м. н., доцент
https://orcid.org/0000-0002-8943-9604
[1]**Яцюк Світлана Миколаївна**, к. пед. наук, доцент
https://orcid.org/0000-0002-8369-6060
[2]**Кузьмич Олена Іванівна**, к. ф.-м. н., доцент
https://orcid.org/0000-0002-8717-4497
[2]**Багнюк Наталія Володимирівна**, к. т. н., доцент
https://orcid.org/0000-0002-7120-5455
[2]**Чернящук Н.Л.,** д. п. н., професор
https://orcid.org/0000-0002-3178-8377
[1]Волинський національний університет імені Лесі Українки, м. Луцьк, Україна
[2]Луцький національний технічний університет, м. Луцьк, Україна

АНАЛІЗ ВИМОГ ТА МЕТОДОЛОГІЯ ПІДБОРУ ТЕМ ДЛЯ ВИВЧЕННЯ ОСНОВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Глинчук Л.Я., Яцюк С.М., Кузьмич О.І., Багнюк Н.В., Чернящук Н.Л. Аналіз вимог та методологія підбору тем для вивчення основ криптографічного захисту інформації. Розглянуто та проаналізовано вимоги та особливості викладання курсу «Криптографічний захист інформації». Проведено методологічний аналіз доцільності та актуальності врахування вказаних особливостей та вимог при викладанні відповідного навчального курсу, дано рекомендації як правильно орієнтуватися у виборі тем та чим керуватися. Складено та обґрунтовано основний перелік тем, згідно якого можна можна варіювати методику викладання в залежності від кількості годин, що даються на вивчення даного курсу та наявності у освітньо-професійній програмі додаткових предметів цього напряму.
Ключові слова: захист інформації, основи криптографічного захисту, криптографічні методи захисту інформації, криптографічний шифр, криптографічний алгоритм.

Глинчук Л.Я., Яцюк С.М., Кузьмич Е.И., Багнюк Н.В., Чернящук Н.Л. Анализ требований и методология подбора тем для изучения основ криптографической защиты информации. Рассмотрены и проанализированы требования и особенности преподавания курса «Криптографическая защита информации». Проведен методологический анализ целесообразности и актуальности учета указанных особенностей и требований при преподавании соответствующего учебного курса, даны рекомендации как правильно ориентироваться в выборе тем и чем руководствоваться. Составлен и обоснован основной перечень тем, согласно которому можно варьировать методику преподавания в зависимости от количества часов, которые даются на изучение данного курса и наличии в образовательно-профессиональной программе дополнительных предметов этого направления.
Ключевые слова: защита информации, основы криптографической защиты, криптографические методы защиты информации, криптографический шифр, криптографический алгоритм.

Glinchuk L.Ya., Yatsyuk S.M., Kuzmych O.I., Bahniuk N.V., Chernyashchuk N.L. Requirements analysis and methodology of selection of topics for studying the basics of cryptographic protection of information. The requirements and features of teaching the course "Cryptographic protection of information" are considered and analyzed. The methodological analysis of expediency and urgency of taking into account the specified features and requirements at teaching of the corresponding training course is carried out, recommendations on how to be correctly guided in a choice of subjects and what to be guided are given. The main list of topics has been compiled and substantiated, according to which it is possible to vary the teaching methods depending on the number of hours given for the study of this course and the availability of additional subjects in this educational and professional program.
Keywords: information protection, basics of cryptographic protection, cryptographic methods of information protection, cryptographic cipher, cryptographic algorithm.

Постановка проблеми та аналіз досліджень. При підготовці фахівців у галузі захисту інформації виділяють такі основні гілки захисту: організаційний захист, програмний захист, апаратний (технічний) захист, інженерний захист, програмно-апаратний захист, криптографічний захист та захист з використанням нормативно-правової бази захисту інформації України. Можна виділити або об'єднати дані гілки захисту по іншому, та суть лишається такою ж. З визначенням, аналізом та врахуванням загроз, їх масштабами, стає зрозуміло, чому такий напрям як «Кібербезпека» виділився як окрема спеціальність. Зрозуміло, що кожна гілка захисту вирішує низку своїх проблем та захищає від притаманних їй загроз.

Як бачимо, свою особливу роль в цьому має і криптографічний захист інформації. Використання криптографічних методів не є новим у напрямі захисту. Якщо подивитися та

дослідити історію виникнення криптографії та використання її методів, то вона заводить дуже далеко в давнину: від стародавніх скитал та найперших форм тайнопису до створення та розробки сучасних апаратних, програмно-апаратних, програмних засобів та комплексів для захисту на основі криптографічних методів. Особливість ще і в тому, що всі не прості методи криптографічного захисту інформації потребують значних ресурсних затрат і не завжди виправдані, хоча в сучасному автоматизованому світі з використанням надшвидкого програмного, апаратного забезпечення або комплексу, даний аспект не завжди відчувається. Все ж таки, варто розуміти в яких випадках доцільно використовувати методи та засоби криптографічного захисту інформації, а в яких не потрібно. До прикладу, криптографічні методи та засоби варто застосовувати до інформації, яка носить характер комерційно-економічної чи державної таємниці.

Такі науковці як І. Берник, І. Громико, В. Кельтон, Д. Леонов, А. Лоу, В. Матвеєв, І. Медвєдовський, В. Носов, П. Орлов, П. Сем'янов, Ю. Харін та ін. приділяють велику увагу проблемам впровадження вивчення сучасних засобів та видів захисту інформації для підготовки майбутніх фахівців у цій галузі. [1]

Про науковців криптографічного захисту можна говорити починаючи з таких відомих людей, які поклали свої дослідження в основу, як Чарльз Беббідж, Клод Шеннон, Керкгофф, Вітфілд Діффі, Мартін Хелман та багато інших видатних людей. Бурхливий розвиток випав на 19, 20 століття, коли розпочалися процеси автоматизації та перехід до сучасної комп'ютерної техніки. Цікавими є дослідження у напрямі криптографії з появою квантових комп'ютерів. Такі науковці як Шор, Гровер, Пауль, Фейнман Дойтч та інші, показали, що можуть виникнути великі загрози забезпечення криптографічної стійкості розроблених та досліджених раніше криптографічних алгоритмів. Крім цього, активні дослідження ведуться у напрямі квантових протоколів та квантових генераторів випадкових послідовностей. Якщо спочатку криптографічні методи в основному будувалися на лінгвістичних схемах, то зараз сучасна криптографія успішно використовує математичний апарат, теорію ймовірностей, теорію інформації, теорію чисел, абстрактну алгебру та багато інших напрямів. Та звичайно, що у сучасних дослідників та науковців є набагато більше можливостей у цій сфері. Деталізація вивчення криптографії призвела до появи нових напрямів у дослідженнях. З появою сучасних пристроїв для обробки, пошуку та зберігання інформації виявилося і надто багато сучасних загроз, яким треба і можна протидіяти з використанням криптографічного захисту.

З описаного вище, стає зрозуміло чому на даний час, кожен викладач, який викладає дисципліни, що так чи інакше стосуються криптографічного захисту інформації, стикається з проблемою оптимального вибору тем для подачі та вивчення матеріалу. Потрібно врахувати багато специфіки та правильно виділити те, що важливо та необхідно подати для студентів, майбутніх фахівців у галузі захисту інформації.

Метою дослідження є детальний аналіз вимог та обґрунтування вибору тем для вивчення основ криптографічного захисту при підготовці майбутніх фахівців у галузі захисту інформації.

Виклад основного матеріалу. Для того, аби оптимально підібрати перелік тем, кожному викладачу потрібно провести багато годин за дослідженням власне самої суті предмету, опрацювати велику кількість літератури та інформаційних джерел, визначити особливості предмету, напрями сучасного розвитку, перспективи на майбутнє, актуальність та необхідність для студентів і т.д.

Але в сучасних реаліях викладання та підготовки потрібно ще і врахувати дуже багато інших вимог та особливостей при формуванні курсу, а саме:

- на якій спеціальності навчаються студенти, майбутні фахівці галузі;
- які предмети були прочитані до викладання курсу основи криптографічного захисту інформації;
- які загальні та фахові компетентності повинні забезпечуватися даним курсом;
- які програмні результати повинен покривати курс;
- згідно якої освітньо-професійної програми треба планувати виклад матеріалу;

- скільки кредитів/годин дається на вивчення курсу;
- можливість матеріально-технічної бази закладу вищої освіти у якій вивчається курс.

Першою особливістю є спеціальність студентів, до прикладу студентам гуманітарних напрямів деталізація та заглиблення у математику, теорію ймовірностей та інші, не підійде та і цікаво не буде, навпаки, для студентів фізичного, математичного та ІТ напряму потрібно та і можливо розглядати все з точки зору математичного апарату та можливістю самим пробувати розробляти та науково обґрунтовувати свої ж власні моделі чи алгоритми криптографічного захисту.

Обов'язковим фактором для врахування є вивчення питання, які предмети передують курсу основи криптографічного захисту інформації для того, аби розуміти рівень викладання. Тобто чи можна деталізовано розглядати методи та алгоритми криптографічного захисту, до прикладу симетричний алгоритм блочного шифрування AES містить складну математичну теорію: операції в полях Галуа, арифметику многочленів, матриці і т.д. Багато криптографічних алгоритмів містять модулярну арифметику, діофантові рівняння та ін. Основою ж кожного алгоритму криптографічного захисту є робота з двійковою системою числення. Важливо звернути увагу на якому рівні студенти вміють програмувати та якими мовами програмування володіють, оскільки, є мови програмування у яких потрібно прописувати всі операції та деталі в ручну, а є мови програмування з уже готовими реалізованими частинами (бібліотеками) деяких алгоритмів шифрування. Можливість чи не можливість та складність візуального програмування для кращої демонстрації процесу шифрування, визначення складності та часу.

Розглядаючи детальніше особливість викладання основ криптографічного захисту для студентів спеціальності «Кібербезпека», потрібно зосередити увагу на законодавчих документах України, виходячи з яких, можливо зробити висновок як правильно побудувати структуру курсу. Отож, до 2018 року такими орієнтирами можна вважати документи: Національний класифікатор України: "Класифікатор професій" ДК 003:2010 // Видавництво "Соцінформ". - К.: 2010, Наказ Міністерства економічного розвитку і торгівлі України від «Про затвердження зміни до національного класифікатора України ДК 003:2010» від 18.11. 2014 р. № 1361 (зміна № 2), "Галузевий стандарт вищої освіти України. Освітньо-професійна програма підготовки", 2010 рік, вибираючи для спеціальності 125 «Кібербезпека». Де прописано код та назва груп професій, код та професійна назва роботи, знання та вміння яким повинен відповідати фахівець. Після появи стандарту вищої освіти за спеціальністю 125 «Кібербезпека» [4] у 2018 році, знання та вміння описуються по іншому, а саме, потрібно вибрати загальні та фахові компетентності, яких дозволить набути курс, до прикладу, пов'язаний з криптографічним захистом інформації, але це актуально і для інших дисциплін. Важливим є вибір програмних результатів навчання, яким повинен задовольняти курс. В даному випадку деталізовано тем курсу теж не вказано, але викладач має можливість підібрати теми таким чином, щоб задовольняти відповідні загальні, фахові компетентності та результати навчання.

Звичайно, що головний документ, на який орієнтується викладач при підготовці курсу є відповідна освітня програма для відповідної спеціальності та відповідного року. Освітньо-професійна програма враховує всі особливості галузі знань та спеціальності, написана та побудована згідно відповідних нормативних документів на той період та відображає специфіку спеціальності. Паралельно до освітньо-професійної програми в допомогу викладачу є навчальний план, де можна зорієнтуватися у послідовності викладу усіх предметів, зрозуміти які предмети йдуть перед курсом викладача, які йдуть після.

До прикладу, якщо в освітньо-професійній програмі, немає більше похідних курсу, що стосуються криптографічного захисту інформації, то викладач, враховуючи це, повинен по максимуму дати інформації, щоб охопити напрям криптології. Напрямами криптології можна вважати ще і стеганографію, криптоаналіз, квантову криптографію, криптографічні протоколи. Хоча предмет і не називається криптологія, обов'язково потрібно дати поняття хоч

і коротко, про зазначені похідні напрями, без цього не буде сформовано цілісного та системного бачення такого виду захисту.

Але якщо освітньо-професійна програма передбачає вивчення у студентів таких предметів як стеганографічний захист, криптоаналіз, криптографічні протоколи, то відповідно до цього, викладач повинен та може змінити зміст курсу основи криптографічного захисту.

Ще одним особливим фактором, який дуже впливає на якість та повноту викладу матеріалу курсу, звичайно є кількість годин, які даються на вивчення, від цього залежить і можливість розгорнути або скоротити запланований матеріал. Зрозуміло, що при більшій кількості годин, можна краще та якісніше дати можливість опанувати курс. З досвіду помітно, що віддаючи великий відсоток матеріалу на самостійне вивчення студентам, вони його в таких масштабах не вивчають та не розглядають, створюючи таким чином для себе прогалини в даному напрямі. Зрозуміло, що при малій кількості годин і при тому, що похідних предметів немає, матеріал повинен охопити все, що стосується напряму криптології і дати розуміння основних понять, методів, алгоритмів, засобів. Виявити у студентів зацікавлення та бажання досліджувати детальніше самостійно.

Матеріально-технічна база закладу вищої освіти, якби не хотілося викладачу від цього залежати, дуже істотно впливає, знову ж таки, на якість та можливість вивчення певних тем криптографічного захисту інформації. Специфікою вивчення даного курсу є можливість роботи з відповідним програмним, апаратним, програмно-апаратним забезпеченням чи комплексами захисту, які працюють на основі криптографічних методів захисту інформації. Що стосується програмного забезпечення, тут простіше – можна використати для демонстрації безкоштовне (відкрите) ПЗ, але до прикладу, при створені цифрового підпису, потрібно працювати з центрами сертифікації ключів, які не дають безкоштовних послуг, крім ПриватБанку, за умови наявності картки банку та ін. Можна скористатися програмним забезпеченням, що дає можливість спробувати його в роботі, а тоді купити ліцензію, проте і тут є мінус – не працюють усі заявлені функції, версія обмежена. Як допомога або виняток, можна скористатися програмним забезпеченням розробленим студентами у вигляді емуляторів того чи іншого алгоритму шифрування та дешифрування, проте таке програмне забезпечення не розроблене для кожного методу і правильність його роботи нічим не підтверджена. Не потрібно забувати і про сучасні онлайн засоби для демонстрації роботи криптографічних методів, до прикладу, подивитися як відбувається хешування за вибраною хеш-функцією можна, використавши ресурс https://www.convertstring.com/ru/Hash, аналогічних ресурсів є декілька. Але ліцензійне програмне забезпечення, яке дає можливість спробувати роботу з криптографічними методами у всій повноті та правильності функціонування є обов'язковою умовою при вивченні курсу. Що стосується апаратного забезпечення (чи комплексів) тут ситуація набагато складніша, бо прилади не коштують дешево, якщо взяти цілісні системи, то вони вартують великих грошей. Тому можуть використовуються прилади, до яких дає доступ заклад вищої освіти. Найкращим варіантом для навчання студентів у сфері захисту інформації є створення та функціонування лабораторій захисту інформації з наявністю в них спеціалізованих пристроїв та програмного забезпечення. До прикладу, можна подивитися за посиланням перелік засобів криптографічного захисту інформації, які мають експертний висновок за результатами державної експертизи у галузі криптографічного захисту інформації:

http://195.78.68.84/dsszzi/control/uk/publish/article?art_id=316570&cat_id=72110&mustWords=%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B8%D0%B9+%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82+%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97&searchPublishing=1

Звичайно, що дотримання таких особливостей та вимог повинна контролювати система внутрішнього забезпечення якості освіти кожного закладу вищої освіти.

Отож, з врахуванням вищеописаних та визначених вимог, все таки, кожен викладач пробує побудувати кістяк або класичну схему курсу, від якої можна рухатися в ту чи іншу

сторону в разі збільшення чи зменшення кількості годин та наявності похідних предметів, у яких може бути вивчено ті чи інші теми.

Опишемо та розглянемо оптимально можливий вибір тем для студентів спеціальності у сфері захисту інформації при невеликій кількості годин та без наявності в освітньо-професійній програмі похідних (паралельних) курсів у сфері криптології.

Для початку, коротко розглянемо, що ж це за така наука криптографія. Існує багато джерел, які дають зрозумілі визначення цього напряму захисту інформації починаючи з Вікіпедії, або до прикладу як у [2]. Але повернімося на початок, потрібно розуміти поняття криптології як науки. Чому криптологія, бо криптологія – наука, яка поділяється на дві: криптографію – досліджує методи шифрування та криптоаналіз – досліджує методи дешифрування інформації. У яке б джерело не дивитися суть означення така ж, до прикладу як у [3].

При дослідженні вибору тем потрібно проаналізувати історію науки, напрями сучасного розвитку, щоб побачити картину цілісно, тоді потрібно перейти до деталізації. Оскільки, розглядаємо випадок при невеликій кількості годин та при відсутності паралельних курсів даної тематики – доведеться будувати схему, яка охоплює по можливості всі елементи.

Звичайно, що логічно і необхідно виділити для початку тему «історія криптографії та основні поняття», проаналізувати з чого почали і до чого прийшли, виділити напрями розвитку, розглянути основні поняття, задати напрям для подальшого вивчення.

Наступним логічним викладом є «законодавство України у сфері криптографічного захисту». Варто розглянути наступні документи: Положення про порядок здійснення криптографічного захисту інформації в Україні (https://zakon.rada.gov.ua/laws/show/505/98#Text), Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису (https://zakon.rada.gov.ua/laws/show/z0868-99#Text) як обов'язкові. Детальніше, за посиланням https://cip.gov.ua/ua/news/perelik-aktiv-zakonodavstva-u-sferi-kriptografichnogo-zakhistu-informaciyi зібрано перелік актів законодавства у сфері криптографічного захисту, яке можна дати для самостійного ознайомлення.

Вирішення проблеми інформаційної безпеки в Україні регламентують: Закон України «Про державну таємницю», Закон України «Про Національну програму інформатизації», Закон України «Про Концепцію Національної програми інформатизації», Закон України «Про електронні документи та електронний документообіг», Закон України «Про електронний цифровий підпис», Закон України «Про захист інформації в автоматизованих системах». [1] Перераховані документи теж можна подати на розгляд самостійно.

Аналізуючи літературу [5, 6, 7, 8] та багато інших джерел, стає зрозуміло, що можна йти різним шляхом вибору тем далі.

Отож, у [5,7] вказано на те, що можна розглядати тему «криптографічні протоколи», проте в інших джерелах розглядають класичні шифри згідно історії розвитку. Історія каже про поділ шифрів на симетричні та асиметричні. Тому, скоріше за все, логічно буде йти за етапами розвитку і розглянути «класичні симетричні алгоритми шифрування» починаючи від найпростіших і завершуючи стандартами шифрування. До прикладу, можна окремо розглянути блокові та потокові симетричні алгоритми (шифри перестановки, заміни, шифри, що використовують аналітичні перетворення, шифри з використанням гамування і т.д.), а також розглянути українські досягнення у цій темі. Як приклади, також проаналізувати такі стандарти симетричних алгоритмів шифрування як DES, AES, ГОСТ. Для детального аналізу складних алгоритмів шифрування потрібен математичний апарат, який можна розглянути додатково в процесі вивчення.

Наступною темою можна запропонувати розглянути «асиметричні алгоритми шифрування та основні поняття цього напряму». Доцільно, знову ж таки спиратися на класику, а саме, вибрати для аналізу алгоритм з відкритим ключем RSA, Діффі-Хелмана, Ель-Гамаля

та ін. За цією темою логічно буде розглянути тему «схеми ідентифікації, автентифікації та криптографічні протоколи».

Особливу роль у вивченні криптографічного захисту інформації відіграють так звані «криптографічні хеш (геш)-функції». Особливістю яких є перетворення вхідних даних будь якого розміру у дані фіксованого розміру. До таких функцій саме криптографічного характеру висувається ряд вимог. Можна проаналізувати та розглянути такі відомі функції як MD2, MD4, MD5, сімейство SHA, N-Hash та інші.

Одним з цікавих прикладів практичного застосування симетричного та асиметричного напряму шифрування є електронний цифровий підпис, тому логічно розглянути тему «електронний цифровий підпис та його різновиди». Алгоритми ЕЦП засновані на базових стандартах, наприклад, таких як RSA, ElGamal та ін. Якщо розглядати ЕЦП, які засновані на еліптичних кривих, зокрема на ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002 (український стандарт ЕЦП). Звідси слідує, що обов'язковою темою для вивчення, яка має передувати цій, повинна бути тема «криптографія на еліптичних кривих».

Як було уже сказано, у випадку не передбачення в освітньо-професійній програмі предметів стеганографічний захист та криптоаналіз, можна в цей перелік добавити теми: «основи стеганографічного захисту» та «елементи криптоаналізу та його види». Розглянути основні напрями та методи стеганографії, в елементах криптоаналізу варто також показати приклад найпростішого криптоаналізу.

Ще одним практичним використанням криптографії є розвиток критовалюти, яка пережила недавній бум, тому можна також запропонувати до викладу тему «особливості криптовалют та законодавство країн світу у їх використанні». Розгорнуто розглядати чи ні, тут на вибір викладача і орієнтація на години, проте цікавий напрям у криптографії, який студенти швидше розглянуть самостійно. Напевно мало таких студентів в галузі ІТ, які б не поцікавився даним напрямом до сьогодні.

На вибір викладача також лишається тема «квантова криптографія», оскільки в основу покладено методи квантової механіки, то для вивчення та аналізу потрібно володіти спеціалізованим матеріалом.

І нарешті, тема, яка теж може бути винесена на самостійний розгляд студентів – «міжнародні та українські стандарти у сфері криптографічного захисту інформації». Даних стандартів є доволі багато, і увагу потрібно зосередити саме на стандартах криптографічного захисту. Іншим цікавим стандартом є Оранжева книга (стандарт міністерства оборони США), що є основою «веселкових публікацій». Пізніше замінено на стандарт критеріїв інформаційної безпеки. Доречніше, можливо було б, цей стандарт розглядати в загальному предметі по захисту інформації або під час детального розгляду нормативно-правової бази спеціальності.

Як бачимо, криптографічний захист інформації досить розвинений, досліджений, опрацьований та актуальний напрям, хоча в перспективі все складніше досліджувати та доводити ефективність нових створених методів. Звичайно, що можна міняти перелік тем, розширювати чи звужувати. Кожен викладач бачить по своєму системну та цілісну картину викладу матеріалу та враховує відповідні вимоги. Тому даний перелік тем є лише приблизним та запропонованим як один з варіантів.

Висновки. Детально розглянуто вимоги та особливості, які можуть бути враховані, при розробці та проведені занять з курсу основи криптографічного захисту. Складено варіант вибору відповідних тем курсу, які можна варіювати та подавати на самостійне вивчення для студентів. Зрозуміло, що ту чи іншу тему можна при необхідності деталізувати чи скорочувати.

Важливо пояснювати, щоб студенти розуміли, що використовуючи тільки криптографічний захист інформації, який би метод не лажав в основі та з якою криптографічною стійкістю, найкращого захисту можна досягти застосовуючи лише всі ланки захисту в сукупності.

Список бібліографічного опису

1. Воскобойніков С.О. Теоретичні та методичні основи застосування криптографічних методів захисту інформації у професійній підготовці майбутніх інженерів-педагогів. ISSN 2075-146X. Витоки педагогічної майстерності. Збірник наукових праць. Полтава, 2011. – С. 79-84.
2. Горобцов В.О. Криптографічний захист інформації. [Електронний ресурс] – Режим доступу: http://esu.com.ua/search_articles.php?id=1575
3. Сушко С.А. Лекція, Практична криптологія. [Електронний ресурс] – Режим доступу: https://bit.nmu.org.ua/ua/student/metod/cryptology/%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D1%8F%201.pdf
4. Наказ Міністерства освіти і науки № 1074 від 04.10.2018 «Про затвердження стандарту вищої освіти за спеціальністю 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти». [Електронний ресурс] – Режим доступу: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf
5. Брюс Шнайєр, Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. – 2-е издание. – М.: Диалектика, 2003. – 610 с. – ISBN: 5-89392-055-4
6. Фергюсон, Нильс, Шнайер, Брюс. Практическая криптография.: Пер. с англ. – М.: Издательський дом «Вильямс», 2005. – 424 с.: ил. – Парал. тит. англ. ISBN 5-8459-0733-0 (рус.)
7. Романьков В.А. Введение в криптографию. Курс лекций. 2-е изд., исправ. – М.: ФОРУМ, 2012. – 240 с. – (Высшее образование). – ISBN: 9785911345730
8. Ященко В.В. Введение в криптографию. Под общей ред. В. В. Ященко. – 4 изд., доп. – М.: МЦНМО, 2012. – 348 с. – ISBN 978-5-4439-0026-1.

References

1. Voskoboynikov S.O. Theoretical and methodical bases of application of cryptographic methods of information protection in professional training of future engineers-teachers. ISSN 2075-146X. The origins of pedagogical skills. Collection of scientific works. Poltava, 2011. - P. 79-84.
2. Gorobtsov V.O. Cryptographic information protection. [Electronic resource] - Access mode: http://esu.com.ua/search_articles.php?id=1575
3. Sushko S.A. Lecture, Practical cryptology. [Electronic resource] - Access mode: https://bit.nmu.org.ua/ua/student/metod/cryptology/%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D1 % 8F% 201.pdf
4. Order of the Ministry of Education and Science № 1074 of 04.10.2018 "On approval of the standard of higher education in the specialty 125 Cybersecurity for the first (bachelor's) level of higher education". [Electronic resource] - Access mode: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf
5. Bruce Schneier, Applied Cryptography. Protocols, algorithms and source texts in the language of S. - 2nd edition. - M .: Диалектика, 2003. - 610 c. - ISBN: 5-89392-055-4
6. Ferguson, Niels, Schneier, Bruce. Practical cryptography .: Per. with English - M .: Williams Publishing House, 2005. - 424 p .: ill. - ISBN 5-8459-0733-0 (rus.)
7. Romankov V.A. Introduction to cryptography. Course of lectures. 2nd ed., Corrected. - M .: FORUM, 2012. - 240 p. - (Higher education). - ISBN: 9785911345730
8. Yashchenko V.V. Introduction to cryptography. Under the general editorship. V.V. Yashchenko. - 4th ed., Ext. - M .: MCNMO, 2012. - 348 p. - ISBN 978-5-4439-0026-1.